

# Interference Search

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	888	((encrypt\$4 or decrypt\$4 or cipher\$4 or cryptograph\$4) with (process\$4 or apparatus or method or system or hardware) with (status or register or check or alert or condition or flag)).clm.	US-PGPUB	OR	ON	2006/09/19 09:48
L2	794	((encrypt\$4 or decrypt\$4 or cipher\$4 or cryptograph\$4) with (interrupt\$3 or interupt\$3 or stop\$3 or break\$3 or halt\$3 or standbye or wait43 or during or duration)).clm.	US-PGPUB	OR	ON	2006/09/19 09:49
L3	124	L1 and L2	US-PGPUB	OR	ON	2006/09/19 09:49
L4	52	L3 and @ad<"20021206"	US-PGPUB	OR	ON	2006/09/19 10:01
L5	26	L4 and (set or element or group or string).clm.	US-PGPUB	OR	ON	2006/09/19 09:50
L6	24	L5 and (twor or multiple or many or more or first or second or third or fourth or next).clm.	US-PGPUB	OR	ON	2006/09/19 09:51
L7	21	L6 and (memory or stor\$3 or keep\$3 or maintain\$3 or save or saving).clm.	US-PGPUB	OR	ON	2006/09/19 09:59
L8	59	((MAC or (message with authentication with code)) with (encrypt\$4 or decrypt\$4 or cipher\$4 or cryptograph\$4) with (generat\$3 or making or make or calucalat\$3 or fabricat\$3 or design\$3)).clm.	US-PGPUB	OR	ON	2006/09/19 10:01
L9	21	L8 and @ad<"20021206"	US-PGPUB	OR	ON	2006/09/19 10:01

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	268	380/37.ccls. and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L2	0	("6408074").URPN.	USPAT	OR	ON	2006/09/19 08:59
L3	6543	encrypt\$5 and decrypt\$5 and cipher\$6	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L4	236254	((data or plaintext or text) near4 block) or datablock	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L5	5535017	receiv\$5 or request45 or quen\$5 or query\$5 or schedul\$5 or interfac\$5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L6	8438518	next or second or subsequent or follow\$5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L7	6815037	operation or block	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L8	54304	MAC or (message near4 authent\$6 near4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L9	347011	((data or plaintext or text) with block) or datablock	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L10	6311	(encrypt\$5 or decrypt\$5 or cipher\$6) with L9	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59

## EAST Search History

L11	35105	(encrypt\$5 or decrypt\$5 or cipher\$6) with L5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L12	6853	L6 with L11	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L13	755	cipher\$5 near4 block\$4 near4 chain\$5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L14	1	("6324288").URPN.	USPAT	OR	ON	2006/09/19 08:59
L15	400	(message near4 authent\$6 near4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L16	6	L15 and plaintext and L13	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 09:07
L17	4	L16 and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L18	17	("6115601").URPN.	USPAT	OR	ON	2006/09/19 08:59
L19	2	("5673319").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/19 08:59
L20	24	("5673319").URPN.	USPAT	OR	ON	2006/09/19 08:59
L21	7	("6226742").URPN.	USPAT	OR	ON	2006/09/19 08:59
L22	1	"5673319".PN.	USPAT; USOCR	OR	ON	2006/09/19 08:59
L23	24	("5673319").URPN.	USPAT	OR	ON	2006/09/19 08:59
L24	400	(message near4 authent\$6 near4 code)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59

## EAST Search History

L25	10	((("5615264") or ("5631960") or ("5796836") or ("5673319") or ("6161183"))).PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/19 08:59
L26	129	"5615264" "5631960" "5796836" "5673319" "6161183"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L27	80	L26 and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L28	1	"19724072"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L29	129	"5615264" "5631960" "5796836" "5673319" "6161183"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L30	80	L29 and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L31	1	"19724072"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L32	10	((("5615264") or ("5631960") or ("5796836") or ("5673319") or ("6161183"))).PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/19 08:59
L33	2	("6760439").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/19 08:59
L34	11	(CBC and MAC).ab.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59

## EAST Search History

L35	83	(L32 or L30 or L33 or L34)and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L36	82	L35 and (CBC or cipher\$5 or encrypt\$5 or decrypt\$5 or block\$5 or chain\$5 or MAC or authenticat\$5 or interrupt\$5 or quene\$5 or receiv\$5 or request\$5 or status or memory or stor\$5 or feedback\$5 or selector\$5)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L37	0	("6453415").URPN.	USPAT	OR	ON	2006/09/19 08:59
L38	2	("6449720").URPN.	USPAT	OR	ON	2006/09/19 08:59
L39	13	("5796836").URPN.	USPAT	OR	ON	2006/09/19 08:59
L40	13	("5796836").URPN.	USPAT	OR	ON	2006/09/19 08:59
L41	536	encrypt\$5 with interrupt\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L42	17179	messag\$5 with authenticat\$5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L43	3370	(encrypt\$5 or decrypt\$5 or cipher\$5) with status	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L44	1133	(encrypt\$5 or decrypt\$5 or cipher\$5) with (feedback\$5 or loopback\$5)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L45	784	cipher\$5 with block\$5 with chain\$5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L46	41	L41 and L45	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59

## EAST Search History

L47	41	L46 and (memory or buffer)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L48	5	L47 and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L49	756	(encrypt\$5 or decrypt\$5 or cipher\$5) with interrupt\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L50	46	L49 and L45	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L51	2	L50 and @ad<"20000114" and (L49 same (stor\$5 or memory or buffer\$5))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L52	1216	parallel with (encrypt\$5 or cipher\$5)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L53	89	L45 and L52	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L54	29	L53 and @ad<"20000114"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L55	4	((("6226742") or ("5796836")).PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/19 08:59
L56	784	cipher\$5 with block\$5 with chain\$5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59

## EAST Search History

L57	1216	parallel with (encrypt\$5 or cipher\$5)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L58	89	L56 and L57	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L59	89	L58	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L60	268	380/37.ccls. and @ad<"20000114"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L61	717	380/28.ccls. and @ad<"20000114"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L62	15	(L60 or L61) and L58	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L63	2	"20020181709"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L64	2	("5796836").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/19 08:59

## EAST Search History

L65	1	L64 and (interrupt\$3 or interupt\$3 or stop\$3 or break\$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L66	2	L64 and (piec\$3 or part\$3 or section or segment\$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 08:59
L67	23	(L14 or L16 or L17 or L18 or L19 or L20 or L21 or L22 or L23) and @ad<"20000114"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 09:08
L68	22	(L25 or L32 or L33 or L34 or L38 or L39 or L40 or L46 or L47 or L48) and @ad<"20000114"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 09:09
L69	37	(L50 or L54 or L55 or L63 or L64 or L62 or L65 or L66) and @ad<"20000114"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 09:10
L70	3	(L67 or L68 or L69) and @pd>"20060401"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/19 09:11





Welcome United States Patent and Trademark Office

## Search Results

## BROWSE

## SEARCH

## IEEE XPLORE GUIDE

## SUPPORT

Results for "(((encrypt and parallel)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001))"

Your search matched 8 of 1408155 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.



## » Search Options

[View Session History](#)[New Search](#)

## Modify Search

(((encrypt and parallel)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001)

☐ Check to search only within this results setDisplay Format: ☒ Citation ☐ Citation & Abstract

## » Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

[view selected items](#)[Select All](#) [Deselect All](#)

- ☐ 1. **Pattern-driven automatic program transformation and parallelization**  
Kessler, C.W.;  
[Parallel and Distributed Processing, 1995. Proceedings. Euromicro Workshop on 25-27 Jan. 1995](#) Page(s):76 - 83  
Digital Object Identifier 10.1109/EMPDP.1995.389152  
[AbstractPlus](#) | Full Text: [PDF\(732 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- ☐ 2. **The role of declimated sequences in scaling encryption speeds through parallelism**  
Witzke, E.L.; Pierson, L.G.;  
[Computers and Communications, 1996., Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on 27-29 March 1996](#) Page(s):515 - 519  
Digital Object Identifier 10.1109/PCCC.1996.493680  
[AbstractPlus](#) | Full Text: [PDF\(356 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- ☐ 3. **Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation**  
Yeo, J.-C.; Guo, J.-I.;  
[Vision, Image and Signal Processing, IEE Proceedings- Volume 147, Issue 2, April 2000](#) Page(s):167 - 175  
Digital Object Identifier 10.1049/ip-vis:20000208  
[AbstractPlus](#) | Full Text: [PDF\(1428 KB\)](#) IEE JNL
- ☐ 4. **Encryption techniques for broadcast communication**  
Ohta, K.; Kurihara, S.;  
[Global Telecommunications Conference, 1991. GLOBECOM '91. Countdown to the New Millennium. Featuring a Mini-Theme on: Personal Communications Services 2-5 Dec 1991](#) Page(s):195 - 200 vol.1  
Digital Object Identifier 10.1109/GLOCOM.1991.188383  
[AbstractPlus](#) | Full Text: [PDF\(468 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- ☐ 5. **RSA-based fail-stop signature schemes**  
Susilo, W.; Safavi-Naini, R.; Pieprzyk, J.;  
[Parallel Processing, 1999. Proceedings. 1999 International Workshops on 21-24 Sept. 1999](#) Page(s):161 - 166  
Digital Object Identifier 10.1109/ICPPW.1999.800056  
[AbstractPlus](#) | Full Text: [PDF\(104 KB\)](#) IEEE CNF  
[Rights and Permissions](#)

- ☐ 6. **VLSI Implementation of a high speed block-cipher module**  
Shehata, K.A.; Ali, H.H.; Shaker, N.H.; Morsy, K.M.;  
Circuits and Systems, 2001. MWSCAS 2001. Proceedings of the 44th IEEE 2001 Midwest Symposium on  
Volume 2, 14-17 Aug. 2001 Page(s):572 - 575 vol.2  
Digital Object Identifier 10.1109/MWSCAS.2001.986256  
[AbstractPlus](#) | Full Text: [PDF](#)(185 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ 7. **Concurrent-simulation-based remote IP evaluation over the Internet for system-on-a-chip design**  
Hung-Pin Wen; Chien-Yu Lin; Youn-Long Lin;  
System Synthesis, 2001. Proceedings. The 14th International Symposium on  
2001 Page(s):233 - 238  
[AbstractPlus](#) | Full Text: [PDF](#)(480 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ 8. **A hybrid pipelined path-searching architecture for multiple communications applications**  
Lin, H.-D.; Messerschmitt, D.G.;  
Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE International Conference on  
Volume 5, 23-26 March 1992 Page(s):653 - 656 vol.5  
Digital Object Identifier 10.1109/ICASSP.1992.226511  
[AbstractPlus](#) | Full Text: [PDF](#)(356 KB) IEEE CNF  
[Rights and Permissions](#)

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.org](#)

© Copyright 2006 IEEE – All Rights Reserved





Welcome United States Patent and Trademark Office

Search Results

[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)[SUPPORT](#)

Results for "(((encrypt and break)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001))"

Your search matched 4 of 1408155 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

[e-mail](#)
[printer friendly](#)

## » Search Options

[View Session History](#)[New Search](#)

## Modify Search

[Search](#)
☐ Check to search only within this results set

 Display Format: ☒ Citation ☐ Citation & Abstract

## » Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

[view selected items](#)[Select All](#) [Deselect All](#)

- ☐ 1. **Augmented encrypted key exchange using RSA encryption**  
 Barmawi, A.M.; Takada, S.; Doi, N.;  
Personal, Indoor and Mobile Radio Communications, 1997. 'Waves of the Year 2000'. PIMRC '97., The 8th IEEE International Symposium on  
 Volume 2, 1-4 Sept. 1997 Page(s):490 - 494 vol.2  
 Digital Object Identifier 10.1109/PIMRC.1997.631052  
[AbstractPlus](#) | Full Text: [PDF\(540 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- ☐ 2. **Predictable timestamp under synchronized clocks in a network**  
 Geng-Sheng Kuo; Jing-Pei Lin;  
Information Theory, 1994. Proceedings., 1994 IEEE International Symposium on  
 27 June-1 July 1994 Page(s):68  
 Digital Object Identifier 10.1109/ISIT.1994.394902  
[AbstractPlus](#) | Full Text: [PDF\(60 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- ☐ 3. **The security of Individual RSA bits**  
 Hastad, J.; Naslund, M.;  
Foundations of Computer Science, 1998. Proceedings.39th Annual Symposium on  
 8-11 Nov. 1998 Page(s):510 - 519  
 Digital Object Identifier 10.1109/SFCS.1998.743502  
[AbstractPlus](#) | Full Text: [PDF\(132 KB\)](#) IEEE CNF  
[Rights and Permissions](#)
- ☐ 4. **Wavelet packet methods for multimedia compression and encryption**  
 Pommer, A.; Uhl, A.;  
Communications, Computers and signal Processing, 2001. PACRIM, 2001 IEEE Pacific Rim Conference on  
 Volume 1, 26-28 Aug. 2001 Page(s):1 - 4 vol.1  
 Digital Object Identifier 10.1109/PACRIM.2001.953508  
[AbstractPlus](#) | Full Text: [PDF\(464 KB\)](#) IEEE CNF  
[Rights and Permissions](#)



Welcome United States Patent and Trademark Office

## Search Results

## BROWSE

## SEARCH

## IEEE XPLORE GUIDE

## SUPPORT

Results for "(((cipher and break)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001))"

Your search matched 13 of 1408155 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.



## » Search Options

[View Session History](#)[New Search](#)

## Modify Search

(((cipher and break)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001)

[Search](#) >☐ Check to search only within this results setDisplay Format: ☒ Citation ☐ Citation & Abstract

## » Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

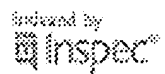
IEEE STD IEEE Standard

[view selected items](#)[Select All](#) [Deselect All](#)

- ☐ 1. **Breaking substitution cyphers using stochastic automata**  
Oommen, B.J.; Zgierski, J.R.;  
[Pattern Analysis and Machine Intelligence, IEEE Transactions on](#)  
Volume 15, Issue 2, Feb. 1993 Page(s):185 - 192  
Digital Object Identifier 10.1109/34.192492  
[AbstractPlus](#) | Full Text: [PDF](#)(660 KB) IEEE JNL  
[Rights and Permissions](#)
- ☐ 2. **Rebuilding the Bombe [Enigma code breaking machine]**  
Lenton, D.;  
[IEE Review](#)  
Volume 47, Issue 6, Nov. 2001 Page(s):7 - 10  
[AbstractPlus](#) | Full Text: [PDF](#)(591 KB) IEE JNL
- ☐ 3. **Cryptanalysis of Krouk's public-key cipher**  
Da Rocha, V.C., Jr; De Macido, D.L.;  
[Electronics Letters](#)  
Volume 32, Issue 14, 4 July 1996 Page(s):1279 - 1280  
[AbstractPlus](#) | Full Text: [PDF](#)(208 KB) IEE JNL
- ☐ 4. **The US Bombes, NCR, Joseph Desch, and 600 WAVES: the first reunion of the US Naval Computing Machine Laboratory**  
Lee, J.A.N.; Burke, C.; Anderson, D.;  
[Annals of the History of Computing, IEEE](#)  
Volume 22, Issue 3, July-Sept. 2000 Page(s):27 - 41  
Digital Object Identifier 10.1109/85.859524  
[AbstractPlus](#) | [References](#) | Full Text: [PDF](#)(192 KB) IEEE JNL  
[Rights and Permissions](#)
- ☐ 5. **The Shannon cipher system with a guessing wiretapper**  
Merhav, N.; Arikan, E.;  
[Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on](#)  
16-21 Aug. 1998 Page(s):83  
Digital Object Identifier 10.1109/ISIT.1998.708668  
[AbstractPlus](#) | Full Text: [PDF](#)(88 KB) IEEE CNF  
[Rights and Permissions](#)
- ☐ 6. **A genetic algorithm for ciphertext-only attack in cryptanalysis**  
Feng-Tse Lin; Cheng-Yan Kao;  
[Systems, Man and Cybernetics, 1995. 'Intelligent Systems for the 21st Century', IEEE International Conference on](#)

Volume 1, 22-25 Oct. 1995 Page(s):650 - 654 vol.1  
Digital Object Identifier 10.1109/ICSMC.1995.537837  
[AbstractPlus](#) | Full Text: [PDF](#)(392 KB) IEEE CNF  
[Rights and Permissions](#)

- ☐ **7. Linearly weak keys of RC5 [private-key cipher]**  
Heys, H.M.;  
[Electronics Letters](#)  
Volume 33, Issue 10, 8 May 1997 Page(s):836 - 838  
[AbstractPlus](#) | Full Text: [PDF](#)(408 KB) IEE JNL
  
- ☐ **8. Nonrandomization: a trial and error cryptanalysis directive**  
Osman, I.M.; Mohamed, H.M.;  
[TENCON 2000. Proceedings](#)  
Volume 3, 24-27 Sept. 2000 Page(s):22 - 24 vol.3  
Digital Object Identifier 10.1109/TENCON.2000.892212  
[AbstractPlus](#) | Full Text: [PDF](#)(204 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **9. Lorenz and Colossus [military cryptography]**  
Sale, A.E.;  
[Computer Security Foundations Workshop, 2000. CSFW-13. Proceedings. 13th IEEE 3-5 July 2000](#) Page(s):216 - 222  
Digital Object Identifier 10.1109/CSFW.2000.856938  
[AbstractPlus](#) | Full Text: [PDF](#)(168 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **10. A new public-key cryptosystem family based on feedback shift registers**  
Diaz, R.G.; Ibanez, M.S.;  
[Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on](#)  
5-7 Oct. 1999 Page(s):318 - 326  
Digital Object Identifier 10.1109/CCST.1999.797931  
[AbstractPlus](#) | Full Text: [PDF](#)(432 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **11. The autoscrtcher and the superscritcher: aids to cryptanalysis of the German Enigma cipher machine, 1944-6**  
Crawford, D.J.; Fox, P.E.;  
[Annals of the History of Computing. IEEE](#)  
Volume 14, Issue 3, 1992 Page(s):9 - 22  
Digital Object Identifier 10.1109/85.150065  
[AbstractPlus](#) | Full Text: [PDF](#)(1180 KB) IEEE JNL  
[Rights and Permissions](#)
  
- ☐ **12. Cryptanalysis of 'nonlinear-parity circuits' proposed at Crypto '90**  
Youssef, A.M.; Taveres, S.E.;  
[Electronics Letters](#)  
Volume 33, Issue 7, 27 March 1997 Page(s):585 - 586  
[AbstractPlus](#) | Full Text: [PDF](#)(232 KB) IEE JNL
  
- ☐ **13. Impact of technology on the defeat of the U-boat September 1939-May 1943**  
Burns, R.W.;  
[Science, Measurement and Technology, IEE Proceedings-](#)  
Volume 141, Issue 5, Sept. 1994 Page(s):343 - 355  
[AbstractPlus](#) | Full Text: [PDF](#)(1384 KB) IEE JNL





Welcome United States Patent and Trademark Office

## Search Results

## BROWSE

## SEARCH

## IEEE XPLORE GUIDE

## SUPPORT

Results for "(((message authentication code)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001)"

Your search matched 18 of 1415139 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

[e-mail](#) [printer friendly](#)

## » Search Options

[View Session History](#)[New Search](#)

## Modify Search

(((message authentication code)&lt;in&gt;metadata)) &lt;and&gt; (pyr &gt;= 1990 &lt;and&gt; pyr &lt;= 2001)

[Search](#)☐ Check to search only within this results setDisplay Format: ☒ Citation ☐ Citation & Abstract

## » Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

[view selected items](#)[Select All](#) [Deselect All](#)

- ☐ 1. **Approximate image message authentication codes**  
Liehua Xie; Arce, G.R.; Graveman, R.F.;  
[Multimedia, IEEE Transactions on](#)  
Volume 3, Issue 2, June 2001 Page(s):242 - 252  
Digital Object Identifier 10.1109/6046.923823  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(276 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- ☐ 2. **On the security of iterated message authentication codes**  
Preneel, B.; van Oorschot, P.C.;  
[Information Theory, IEEE Transactions on](#)  
Volume 45, Issue 1, Jan. 1999 Page(s):188 - 199  
Digital Object Identifier 10.1109/18.746787  
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(332 KB\)](#) IEEE JNL  
[Rights and Permissions](#)
- ☐ 3. **Attacks on MacDES MAC algorithm**  
Coppersmith, D.; Mitchell, C.J.;  
[Electronics Letters](#)  
Volume 35, Issue 19, 16 Sept. 1999 Page(s):1626 - 1627  
Digital Object Identifier 10.1049/el:19991119  
[AbstractPlus](#) | Full Text: [PDF\(236 KB\)](#) IEE JNL
- ☐ 4. **MacDES: MAC algorithm based on DES**  
Knudsen, L.R.; Preneel, B.;  
[Electronics Letters](#)  
Volume 34, Issue 9, 30 April 1998 Page(s):871 - 873  
[AbstractPlus](#) | Full Text: [PDF\(416 KB\)](#) IEE JNL
- ☐ 5. **Chosen-text attack on CBC-MAC**  
Knudsen, L.R.;  
[Electronics Letters](#)  
Volume 33, Issue 1, 2 Jan. 1997 Page(s):48 - 49  
[AbstractPlus](#) | Full Text: [PDF\(292 KB\)](#) IEE JNL
- ☐ 6. **Key recovery attack on ANSI X9.19 retail MAC**  
Preneel, B.; Van Oorschot, P.C.;  
[Electronics Letters](#)  
Volume 32, Issue 17, 15 Aug. 1996 Page(s):1568 - 1569  
[AbstractPlus](#) | Full Text: [PDF\(264 KB\)](#) IEE JNL

- ☐ **7. FPGA Implementation of MD5 hash algorithm**  
Deepakumara, J.; Heys, H.M.; Venkatesan, R.;  
Electrical and Computer Engineering, 2001. Canadian Conference on  
Volume 2, 13-16 May 2001 Page(s):919 - 924 vol.2  
Digital Object Identifier 10.1109/CCECE.2001.933564  
AbstractPlus | Full Text: PDF(372 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **8. Authentication for low power systems**  
Marvel, L.M.; Boncelet, C.G., Jr.;  
Military Communications Conference, 2001. MILCOM 2001. Communications for Network-  
Centric Operations: Creating the Information Force. IEEE  
Volume 1, 28-31 Oct. 2001 Page(s):135 - 138 vol.1  
Digital Object Identifier 10.1109/MILCOM.2001.985777  
AbstractPlus | Full Text: PDF(234 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **9. Trading off strength and performance in network authentication: experience with the ACSA project**  
Adcock, J.M.; Balenson, D.M.; Carman, D.W.; Heyman, M.; Sherman, A.T.;  
DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings  
Volume 1, 25-27 Jan. 2000 Page(s):127 - 139 vol.1  
Digital Object Identifier 10.1109/DISCEX.2000.824971  
AbstractPlus | Full Text: PDF(108 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **10. Efficient commerce protocols based on one-time pads**  
Schneider, M.A.; Felten, E.W.;  
Computer Security Applications, 2000. ACSAC '00. 16th Annual Conference  
11-15 Dec. 2000 Page(s):317 - 326  
Digital Object Identifier 10.1109/ACSAC.2000.898886  
AbstractPlus | Full Text: PDF(720 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **11. Robust Image hashing**  
Venkatesan, R.; Koon, S.-M.; Jakubowski, M.H.; Moulin, P.;  
Image Processing, 2000. Proceedings. 2000 International Conference on  
Volume 3, 10-13 Sept. 2000 Page(s):664 - 666 vol.3  
Digital Object Identifier 10.1109/ICIP.2000.899541  
AbstractPlus | Full Text: PDF(272 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **12. Image enhancement towards soft image authentication**  
Liehua Xie; Arce, G.R.; Lewis, A.; Basch, E.B.;  
Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference on  
Volume 1, 30 July-2 Aug. 2000 Page(s):497 - 500 vol.1  
Digital Object Identifier 10.1109/ICME.2000.869647  
AbstractPlus | Full Text: PDF(360 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **13. Fast checking of individual certificate revocation on small systems**  
Russell, S.;  
Computer Security Applications Conference, 1999. (ACSAC '99) Proceedings. 15th Annual  
6-10 Dec. 1999 Page(s):249 - 255  
Digital Object Identifier 10.1109/CSAC.1999.816034  
AbstractPlus | Full Text: PDF(88 KB) IEEE CNF  
Rights and Permissions
  
- ☐ **14. Multicast security: a taxonomy and some efficient constructions**  
Canetti, R.; Garay, J.; Itkis, G.; Micciancio, D.; Naor, M.; Pinkas, B.;  
INFOCOM '99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications  
Societies, Proceedings. IEEE



Volume 2, 21-25 March 1999 Page(s):708 - 716 vol.2  
Digital Object Identifier 10.1109/INFCOM.1999.751457

[AbstractPlus](#) | Full Text: [PDF](#)(968 KB) IEEE CNF  
[Rights and Permissions](#)

- ☐ **15. Fast authentication codes based on random polynomial residue classes**  
Afanassiev, V.; Smeets, B.; Gehrmann, C.;  
[Information Theory, 1997. Proceedings., 1997 IEEE International Symposium on](#)  
29 June-4 July 1997 Page(s):175  
Digital Object Identifier 10.1109/ISIT.1997.613090  
[AbstractPlus](#) | Full Text: [PDF](#)(100 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **16. A HOL extension of GNY for automatically analyzing cryptographic protocols**  
Brackin, S.H.;  
[Computer Security Foundations Workshop, 1996. Proceedings., 9th IEEE](#)  
10-12 June 1996 Page(s):62 - 76  
Digital Object Identifier 10.1109/CSFW.1996.503691  
[AbstractPlus](#) | Full Text: [PDF](#)(1116 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **17. Graph-based authentication of digital streams**  
Miner, S.; Staddon, J.;  
[Security and Privacy, 2001. S&P 2001. Proceedings, 2001 IEEE Symposium on](#)  
14-16 May 2001 Page(s):232 - 246  
Digital Object Identifier 10.1109/SECPRI.2001.924301  
[AbstractPlus](#) | Full Text: [PDF](#)(1204 KB) IEEE CNF  
[Rights and Permissions](#)
  
- ☐ **18. Header hopping and packet mixers**  
Tschudin, C.F.;  
[Computer Communications and Networks, 2000. Proceedings, Ninth International Conference on](#)  
16-18 Oct. 2000 Page(s):316 - 319  
Digital Object Identifier 10.1109/ICCCN.2000.885508  
[AbstractPlus](#) | Full Text: [PDF](#)(408 KB) IEEE CNF  
[Rights and Permissions](#)

[Help](#) [Contact Us](#) [Privacy & Security](#) [IEEE.org](#)

© Copyright 2006 IEEE – All Rights Reserved

